Discrimination of Unitary Transformations and Quantum Algorithms

David Collins

Department of Physical and Environmental Sciences, Mesa State College, Grand Junction, Colorado, USA

Abstract. Quantum algorithms are typically understood in terms of the evolution of a multi-qubit quantum system under a prescribed sequence of unitary transformations. The input to the algorithm prescribes some of the unitary transformations in the sequence with others remaining fixed. For oracle query algorithms, the input determines the oracle unitary transformation. Such algorithms can be regarded as devices for discriminating amongst a set of unitary transformations. The question arises: "Given a set of known oracle unitary transformations, to what extent is it possible to discriminate amongst them?" We investigate this for the Deutsch-Jozsa problem. The task of discriminating amongst the admissible oracle unitary transformations results in an exhaustive collection of algorithms which can solve the problem with certainty.

ORACLE ALGORITHMS AND DISCRIMINATION OF QUANTUM OPERATIONS

Quantum algorithms [1, 2, 3, 4] are usually solve computational problems with the aid of a binary oracle function $f : \{0,1\}^n \mapsto \{0,1\}^m$, which depends on the problem. The simplest case, where $m = 1$, occurs in the Deutsch-Jozsa [1] and Grover's [4] algorithms. In quantum algorithms a given oracle, f, is invoked via unitary transformation, $\hat{U}_f$, whose structure depends on the nature of the oracle. For example, in both the Deutsch-Jozsa algorithm [5] and Grover's algorithm the oracle is defined on computational basis states, $|x\rangle \equiv |x_n \ldots x_1\rangle$ with $x_i \in \{0,1\}$, to be $\hat{U}_f |x\rangle = (-1)^{f(x)} |x\rangle$ and this is extended linearly to superpositions of computational basis states. The general structure of such oracle algorithms is encapsulated in an algorithm unitary

$$\hat{U}_{\text{alg}} = \hat{V}_M \hat{U}_f \ldots \hat{U}_f \hat{V}_1 \hat{U}_f \hat{V}_0 \tag{1}$$

where $\hat{V}_0, \ldots, \hat{V}_M$ are oracle independent unitary transformations and the oracle is invoked M times. This is applied to a quantum system in an oracle independent initial state $|\Psi_i\rangle$, giving an oracle dependent final state $|\Psi_f\rangle = \hat{U}_{\text{alg}} |\Psi_i\rangle$, upon which a computational basis measurement is performed. It is important to note that *the input to the algorithm is the oracle unitary* and not the initial state. The output from the algorithm potentially identifies the oracle unitary or a class of oracle unitaries. For example, in Grover's algorithm for searching a database one marked item at location s, $f(x) = 0$ whenever $x \neq s$ and $f(s) = 1$. The standard Grover's algorithm terminates in a compu-

tational basis measurement which yields s with high probability. Since the admissible oracles for this problem can be labeled by s, the algorithm *identifies the input oracle unitary* with high probability. We thus regard the quantum algorithm as a tool for discriminating between classes of admissible input oracle unitaries.

The problem of discriminating between unitary transformations is usually reduced to a quantum state discrimination problem [6, 7]. This considers application of one unitary from a collection of known possible unitaries, $\{\hat{U}_1, \hat{U}_2, \ldots\}$, any of which may be invoked with known probabilities $\{p_1, p_2, \ldots\}$. An (unknown) unitary from this collection is selected and can be applied one or more times to a single quantum system, after which a measurement is performed so as to infer the actual unitary used. We consider the case where the *unitary is used once.* This is converted into a standard state discrimination problem [8] by choosing an initial state, described by a density operator $\hat{\rho}_i$, and applying the given unitary, $\hat{U}_j$, to yield an output state $\hat{\rho}_{f\,j} = \hat{U}_j \hat{\rho}_i \hat{U}_j^\dagger$. The problem of discrimination between the unitaries reduces to discrimination between the states $\{\hat{\rho}_{f\,1}, \hat{\rho}_{f\,2}, \ldots\}$. This involves subjecting the system to a POVM with positive operator elements $\{\hat{E}_1, \hat{E}_2, \ldots\}$ that satisfy $\sum_j \hat{E}_j = \hat{I}$ and applying an rule for inferring the state from the measurement outcome (for example, if the measurement yields the outcome associated with $\hat{E}_j$, then the state was $\hat{\rho}_{f\,j}$). This can be converted to an inference about the unitary used and the task is to find the POVM and the initial density operator which maximizes the probability with which the unitary is correctly inferred.

The central idea of this work is to use techniques for discrimination of quantum states or unitaries to arrive at and assess quantum algorithms. In the remainder of this article we focus on the Deutsch-Jozsa algorithm.

APPLICATION TO THE DEUTSCH-JOZSA ALGORITHM

The Deutsch-Jozsa problem considers functions $f : \{0,1\}^n \mapsto \{0,1\}$ which are required to be in one of two possible classes : *constant or balanced.* A constant function returns the same output for all possible arguments while a balanced function returns 0 for exactly half of the possible inputs and 1 for the other half. The problem is to determine the function class with a minimum number of oracle invocations. A classical algorithm that solves with certainty requires $2^{n-1} + 1$ oracle invocations in the worst case [1, 9]. A quantum algorithm for solving this exists [1, 9] and, in its modified form [5], uses the oracle defined on computational basis elements as

$$\hat{U}_f |x\rangle := (-1)^{f(x)} |x\rangle. \tag{2}$$

The question that we pose is whether it is possible to arrive at quantum algorithms that solve the Deutsch-Jozsa problem purely by considering the possibility of discriminating between the oracle unitaries for balanced and constant functions, given by Eq. (2).

Since the Deutsch-Jozsa problem requires that a determination of function class rather than the actual function used, the discrimination problem is one of discriminating between the two classes of unitary transformations. The can be conveniently recast as a problem of discriminating between two quantum operations, one corresponding to the two constant functions and the other to the set of all balanced functions. Generally either

relevant quantum operation can be represented as $\hat{\rho}_i \mapsto \hat{\rho}_f = \sum_{f \text{ in class}} p_f \hat{U}_f \hat{\rho}_i \hat{U}_f^\dagger$ where $\{p_f | f \text{ in class}\}$ are the probabilities with which the various unitaries within each class are applied. The operation for the constant class is independent of these probabilities and performs

$$\hat{\rho}_i \mapsto \hat{\rho}_{f\text{const}} = \hat{\rho}_i. \tag{3}$$

For the balanced class, we consider the case where p_f are identical for all balanced functions. A detailed calculation shows that the operation is

$$\hat{\rho}_i \mapsto \hat{\rho}_{f\text{bal}} = \frac{1}{N-1} \left(-\hat{\rho}_i + N \sum_{x=0}^{N-1} \hat{P}_x \hat{\rho}_i \hat{P}_x \right) \tag{4}$$

where $N = 2^n$ and $\hat{P}_x := |x\rangle \langle x|$. The problem of discrimination between the two classes of unitaries reduces to that of discrimination between the two density operators, $\hat{\rho}_{f\text{const}}$ and $\hat{\rho}_{f\text{bal}}$. Conclusive discrimination between these requires a POVM with two elements $\hat{E}_{\text{const}}$ and $\hat{E}_{\text{bal}} = \hat{I} - \hat{E}_{\text{const}}$. If the measurement outcome associated with $\hat{E}_{\text{const}}$ is obtained, then it will be inferred that the state after the application of the operation is $\hat{\rho}_{f\text{const}}$ and that hence the unitary is one for a constant function; a similar rule applies for the balanced case. The probability with which a correct inference will be made is $\Pr(\text{correct inference}) = p_{\text{const}} \text{Tr}\left(\hat{\rho}_{f\text{const}} \hat{E}_{\text{const}}\right) + p_{\text{bal}} \text{Tr}\left(\hat{\rho}_{f\text{bal}} \hat{E}_{\text{bal}}\right)$ where p_{const} and $p_{\text{bal}} = 1 - p_{\text{const}}$ are the probabilities with which the function is chosen from the constant or balanced classes respectively. The inference will be correct with certainty for arbitrary p_{const} if $\text{Tr}\left(\hat{\rho}_{f\text{const}} \hat{E}_{\text{const}}\right) = 1$ and $\text{Tr}\left(\hat{\rho}_{f\text{bal}} \hat{E}_{\text{bal}}\right) = 1$. The requirement that $\text{Tr}\left(\hat{\rho}_{f\text{const}} \hat{E}_{\text{const}}\right) = 1$ can be shown, via a series of inferences based on the positivity of both $\hat{\rho}_{f\text{const}}$ and $\hat{E}_{\text{const}}$ and the fact that their eigenvalues are each in the range $[0, 1]$, to imply that $\hat{E}_{\text{const}}$ is the identity operator on the support of $\hat{\rho}_{f\text{const}}$ (i.e. the subspace orthogonal to the kernel) and is zero elsewhere. Applying this to the analogous operators for the balanced case yields the result that the supports of $\hat{\rho}_{f\text{const}}$ and $\hat{\rho}_{f\text{bal}}$ are orthogonal or, equivalently

$$\hat{\rho}_{f\text{const}} \hat{\rho}_{f\text{bal}} = \hat{\rho}_{f\text{bal}} \hat{\rho}_{f\text{const}} = 0. \tag{5}$$

Eqs. (3)-(5) imply that

$$\left[\hat{\rho}_i, \hat{\Lambda}\right] = 0 \quad \text{and} \tag{6}$$

$$N \hat{\Lambda} \hat{\rho}_i = \hat{\rho}_i^2. \tag{7}$$

where $\hat{\Lambda} := \sum_{x=0}^{N-1} \hat{P}_x \hat{\rho}_i \hat{P}_x$ and satisfies the requirements for a density operator. Denote the orthonormal basis in which the two operators $\hat{\rho}_i$ and $\hat{\Lambda}$ can be diagonalized simultaneously by $\{|\phi_j\rangle | j = 1, \ldots N\}$. Thus $\hat{\rho}_i = \sum_{j=1}^{M} p_j |\phi_j\rangle \langle \phi_j|$ where M is the number of non-zero eigenvalues of $\hat{\rho}_i$ and $\hat{\Lambda} = \sum_{j=1}^{N} \lambda_j |\phi_j\rangle \langle \phi_j|$. Suppose that $p_1 \neq 0$. Then Eqs. (6) and (7) can be shown to imply that

$$\frac{p_1}{N} = p_1 \sum_x |\phi_1(x)|^4 + \sum_{k \neq 1}^{M} p_k \sum_x |\phi_k(x)|^2 |\phi_1(x)|^2. \tag{8}$$

where $\phi_1(x) = \langle x | \phi_1 \rangle$. The normalized state $|\phi_1\rangle$ satisfies $\sum_x |\phi_1(x)|^2 = 1$ and a Lagrange multiplier technique demonstrates that, subject to this constraint, $\sum_x |\phi_1(x)|^4 \geqslant 1/N$ with equality attained if and only if $|\phi_1(x)|^2 = 1/N$ for all $x = 0, \ldots N - 1$. Thus Eq. (8) implies

$$\frac{p_1}{N} \geqslant \frac{p_1}{N} + \sum_{k \neq 1}^{M} p_k \sum_x |\phi_k(x)|^2 |\phi_1(x)|^2. \tag{9}$$

with equality if and only if $|\phi_1(x)|^2 = 1/N$ for all $x = 0, \ldots N - 1$. Since the second term on the right hand side of Eq. (9) is non-negative, the only possibility is that the equality holds and that $|\phi_1(x)|^2 = 1/N$ for all $x = 0, \ldots N - 1$. This implies that $p_k = 0$ for $k \neq 1$.

Thus the only possible initial states which discriminates conclusively and correctly with certainty between the two classes of quantum operations for the Deutsch-Jozsa problem are $\hat{\rho}_i = |\phi\rangle \langle \phi|$ where

$$|\phi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{i\theta_x} |x\rangle \tag{10}$$

with θ_x arbitrary real phases. The corresponding POVM elements are $\hat{E}_{\text{const}} = |\phi\rangle \langle \phi|$ and $\hat{E}_{\text{bal}} = \hat{I} - \hat{E}_{\text{const}}$. It is easily verified that this algorithm discriminates with certainty between balanced and constant functions regardless of *a priori* probabilities.

CONCLUSION

We have shown that the techniques of unitary discrimination can be applied to yield an exhaustive collection of algorithms which solve the Deutsch-Jozsa problem with certainty. This suggests that it may be fruitful to investigate unitary discrimination in the context of other algorithms or whenever the set of input states is restricted (such as thermal equilibrium states in NMR).

ACKNOWLEDGMENTS

REFERENCES

1. D. Deutsch, and R. Jozsa, *Proc. R. Soc. Lond. A* **439**, 553 (1992).
2. D. R. Simon, *Proceedings 35th Annual Symposium on Foundations of Computer Science* pp. 116–123 (1994).
3. P. Shor, *SIAM J. Comput.* **26**, 1484 (1997).
4. L. K. Grover, *Phys. Rev. Lett.* **79**, 325 (1997).
5. D. Collins, K. W. Kim, and W. C. Holton, *Phys. Rev. A* **58**, 1633 (1998).
6. A. Acín, *Phys. Rev. Lett.* **87**, 177901 (2001).
7. M. F. Sacchi, *Phys. Rev. A* **71**, 062340 (2005).
8. C. W. Helstrom, *Quantum Detectionand Estimation Theory*, Academic Press, New York, 1976.
9. R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, *Proc. R. Soc. Lond. A* **454**, 339 (1998).